#12
6/22/04
A.W.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appeal No. _____

Appellants:	Carl BILICSKA et al.
Application No.:	09/675,399
Group No.:	2175
Filed:	September 29, 2000
Examiner:	Hassan Mahmoudi
For:	AUTOMATED AUTHENTICATION HANDLING SYSTEM

Attorney Docket No.: 29250-001034/US

BRIEF ON APPEAL ON BEHALF OF APPELLANT

BOX APPEAL
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

June 9, 2004

TABLE OF CONTENTS

BRIEF ON BEHALF OF APPELLANT

In support of the Notice of Appeal filed April 15, 2004, appealing the Examiner's final rejections contained in a Final Office Action mailed January 15, 2004 of each of pending claims 1-14 of the present application which appear in the attached Appendix, Appellant hereby provides the following remarks.

I. REAL PARTY IN INTEREST

The present application is assigned to Lucent Technologies Inc., by an Assignment recorded on September 29, 2000, Reel 011176, Frame 0834.

II. RELATED APPEALS AND INTERFERENCES

The Appellant does not know of any appeals or interferences which would directly affect or which would be directly affected by, or have a bearing on, the Board's decision in this Appeal.

III. STATUS OF THE CLAIMS

Claims 1-14 reproduced in the attached Appendix A are the claims on Appeal. Each of these claims is currently pending in the application.

IV. STATUS OF ANY AMENDMENTS FILED SUBSEQUENT TO THE FINAL REJECTION

A Request for Reconsideration dated April 15, 2004 was filed with the U.S. Patent Office in response to the Final Rejection dated January 15, 2004, and was considered and entered by the Examiner.

V. SUMMARY OF THE INVENTION

The present inventions are directed at automated authentication handling systems that allow a user to initiate a single authentication process with one authentication server which, in turn, automatically initiates authentication processes with all other servers in a network where

the user is permitted access. The authentication server further establishes a trusted communication link between the user and at least one of the other servers.

In more detail, with reference to Figure 4 for purposes of illustration, an automated authentication handling system 100 according to the present invention includes a plurality of clients 102-104 that are connected via a network 106 such as the Internet or an intranet. Similarly, a plurality of application servers 108-110 are connected to the network. Advantageously, the present invention includes an authentication server 111 connected to the network 106 and configured to authenticate clients and application servers to establish a communication link 112-114 directly between the clients 102-104 and the application servers 108-110. For purposes of illustrating the features of this invention, the invention will be described in the context of Internet protocols and more particularly the HyperText Transfer Protocols (HTTP). However those skilled in the art will appreciate that the features of this invention may be utilized on any network protocol platform.

The authentication server 111 generally may include conventionally available hardware and software for connecting to a network and interacting with communication protocols used by the network. For example, when used over the Internet the server may include web server software of the type published by Apache Digital Corporation of Durango, CO. The Apache web server software is preferred because it may be easily configured to include specialized tasks using software compatible with the Common Gateway Interface (CGI). The authentication server of the present invention includes two specialized tasks or modules (Figure 5), namely, an identifier engine 116 and a communication initiation engine 118.

With continued reference to Figure 5, the identifier engine 116 includes a database 120 having a plurality of client identifier records 122 and a plurality of application server records 124. Each of the client identifier records is related to one or more of the application servers. The relationships of the client identifier records to the application servers is preferably tailored to the desired relationships between the clients 102-104 and the applications servers 108-110. As a result, for each client identifier in the database a listing of application servers authorized by the client identifier may be generated in a report. When a client provides a client identifier, a report 126 containing a listing of the application servers authenticated for access by the client identifier is generated and sent to the client. The report is preferably generated in a hyper-text format such as the hyper-text markup language (HTML) used by HTTP. The hyper-text format is embedded with a link for each application server in the listing. The link addresses the communication initiator engine on the authentication server and includes a request to establish a communication link with an associated application server. This request is preferably in the form of an HTML POST command in which the application server is provided in the hypertext document in an encrypted format. This prevents a user (client) from modifying the hypertext document to change access privileges.

Accordingly, the hypertext report provides a user interface 128 that may be used by a client when the hypertext document is loaded by a conventional web browser of the type such as Explorer published by Microsoft or Navigator published by Netscape. The user interface 128, when used by a client having a conventional graphical user interface such as Microsoft Windows or Apple Macintosh OS, may appear as a separate window that can be accessed when needed by a user. Using the HTML language it will be appreciated that a number of user interface

configurations may be used including, but not limited to, pull-down menus or hypertext listings. Once the document has been sent to the client, no further authentication by the user is required to access the application servers contained in the listing. This user interface provides a great advance over existing authentication methodologies as the user does not have to provide a separate authentication for each of the application servers. Furthermore, it will be appreciated that authentication administration can be handled by a single server rather than having separate authentication administrators for each of the application servers. A client's communications with the authentication server may include a Secure Socket Layer (SSL) session link, cookies or other conventional security measures that may be used to verify continued communication from the client to the authentication server.

In another embodiment, the client identifier is further related to session assignment information for each of the application servers. The session assignment can include information for limiting client access to the features on each of the application servers as well as session timeout information. It will be appreciated that the session assignment information may be specifically tailored to access the capabilities of each of the application servers. When the report in hypertext format is sent to the client the link designating a request for an application server may be encoded with application server information in an encrypted format.

The communication initiator engine 118 is responsive to a request from the client to establish a communication link 130 with one of the application servers. The communication initiator engine 118 preferably receives the encrypted request information, illustrated by line 132, and decrypts the information. The requested information is preferably compared to a look-up table in which each application server and session assignment information is stored as a separate

listing. The authentication server matches the client's request with the appropriate listing. The listing is combined with the client's address. The client address and session information are then encrypted by the communication initiator engine and transmitted to the application server, illustrated by line 134, again using an HTTP POST.

The application server receives the information transmitted in the post command and includes a verification engine 136, preferably running as a CGI script on the application server. It should be noted that the verification engine 136 does not verify that the information was received by checking the IP address of a trusted authentication server, rather it decrypts the posted information and uses a shared secret data field to verify the authentication server. It will be appreciated by those skilled in the art that such verification allows for dynamic, IP addressing of the authentication server. The encryption/decryption method used by the present invention may vary; however, a public key/private key methodology is preferred. Thus, the decryption of information from the authentication server is decrypted using a private key contained on the application server. The decrypted information includes the session assignment information and the client's address. The information also preferably includes a verification record that contains secret information shared exclusively between the authentication server and the application as a further verification that the information was transmitted from a trusted source. If the verification fails, an error message is returned and no further action is taken.

If the verification is cleared, a Uniform Resource Locator (URL) is generated containing a unique address for the client to access the application and further includes session assignment information that is encrypted by the verification engine prior to transmittal. The URL is then transmitted to the Authentication Server, illustrated by line 140, which in turn forwards the URL

directly to the client, illustrated by line 142. Once received by the client, the URL is addressed back to the application server directly from the client along with the encrypted session information initiating the communication link 134. The application server again decrypts the session information and verifies that the URL request was transmitted from the IP address of the client 102 originally transmitted to the application server by the authentication server. The application server also verifies that a session timeout time is still valid. The application server then establishes a trusted communication link 134 directly with the client. The trusted communication link 134 may include security such as an SSL communications link; or a cookie containing the relevant session information may be placed on the client's computer. The cookie is used by the application to verify the user and provide other information relevant to the session such as session time-out information. The URL then redirects the client to the main session application page of the web site.

With reference to Figure 6, signaling between a client 102 and an application server 108 using an authentication server 108 includes initiating a login request from the client to the authentication server, illustrated by line 125. The authentication server replies with a report in hypertext listing the application servers authorized to be accessed by the client, illustrated by line 126. A client selects an application server for access and submits a request to the authentication server, illustrated by line 132. The authentication server forwards the request to the application server, illustrated by line 134. The application server responds and confirms access as illustrated by line 140. The authentication server forwards the selection authorization to the client 102, illustrated by line 142. The client 102 and application server 108 then establish and communicate via a trusted communication link, illustrated by line 130.

VI. ISSUES PRESENTED

Whether or not claims 1-14 are obvious under 35 U.S.C. §103(a) by the combination of U.S. Patent No. 5,863,325 to Reed et al. ("Reed") in view of U.S. Publication No. 2001/0042107 A1 to Palm ("Palm").

VII. GROUPING OF THE CLAIMS

Appellant respectfully requests, for the purposes of this Appeal, that the grouping of the claims be as follows:

Group I including claims 1-8; and

Group II including claims 9-14.

For purposes of this Appeal, the patentability of the Group I and II claims stand and fall together.

VIII. ARGUMENTS

a) The Rejections

The following summary of the Examiner's rejections is based on the Final Office Action, paper 8 and the Advisory Action mailed on May 31, 2004, paper 11, unless otherwise noted.

The Examiner has rejected claims 1-14 under 35 U.S.C. § 103(a) as being obvious based on the combination of Reed in view of Palm.

Regarding claim 1, paraphrasing the statements made in the Office Action and Advisory Action, the Examiner alleges:

> Reed teaches an automated authentication handling system for use by clients on a network comprising:
>
> an authentication server adapted to establish a two-way trusted communication link for access by an authenticated user to an application server associated with a client identifier;

Reed et al does not teach a list of application servers;

Palm teaches a communications system, in which he teaches a list of application servers;

therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reed et al to include a list of application servers; and

it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reed et al by the teaching of Palm, because including a list of application servers, would provide the user the opportunity of selecting a particular server from a plurality of servers, and would enable the system to route the desirable objects to the designated server, selected from a list of available servers.

b) Reasons Supporting the Allowability of Group I Claims

(Claims 1-8)

With regard to claim 1 from which the remaining claims depend, Appellants assert that claim 1 is not obvious in view of the combination of Reed and Palm. Claim 1 reads as follows:

1. An automated authentication handling system for use by clients on a network comprising:

an authentication server adapted to establish a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier.

As admitted by the Examiner in the Final Office Action, Reed does not disclose or suggest an authentication server which establishes a two-way, trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier. More particularly, the Final Office Action correctly states that Reed "does not teach a list of application servers". This is true, however, Reed is also silent as to an authentication server which establishes "a two-way, trusted communication link" for access by an authenticated user

which enables the user to access a list of application servers which are associated with a client identifier. The excerpts from Reed mentioned in the Final Office Action which allegedly disclose a two-way, trusted communication link do not in fact disclose a two-way, trusted communication link that allows an authenticated user to access a list of application servers associated with a client identifier. At most, the references to Reed (column 76, lines 34-44 and column 81, lines 59-67) disclose a two-way link. There is no discussion or suggestion of the link being a trusted communication link, no discussion or suggestion of the link being established between an authenticated user and an authentication server, and no discussion or suggestion that the two-way link allows an authenticated user access to a list of application servers associated with a client identifier, as in the claims of the present invention. Nor does the addition of Palm overcome these deficiencies.

The relevance that Palm appears to have to the present application is that it discusses the use of multiple servers, referred to as media servers 115. There is no discussion or suggestion in Palm of an authentication server as in the claims of the present invention. The closest Palm comes to a discussion of authentication at all is in paragraphs 92 through 94. In these paragraphs Palm generally discusses that a multi-media device 105 can be authorized to access a media server 115 using a "registration phase" or an "authorized client-based authentication certificate." A fair reading of Palm is that the registration phase and/or authentication certificate involves the multi-media device 105 or the media server 115, neither of which perform the functions of an authentication server. Notably, the gateway 110 which connects the multi-media device 105 to the media server 115 is not disclosed as possessing any kind of authentication capability

whatsoever. In sum, Palm does not disclose or suggest an authentication server, as in the claims of the present invention.

In addition, Palm does not disclose or suggest any device which allows an authenticated user to access a list of application servers associated with a client identifier. Instead, each of the media servers 115 is associated with its own registration phase or authentication certificate. In contrast, the claims of the present invention only require a single client identifier in order to access a list of application servers.

In sum, claim 1 of the present invention would not have been obvious to one of ordinary skill in the art at the time the present application was filed upon reading the disclosure in Reed or Palm, taken separately or in combination, because neither Reed nor Palm discloses or suggests an authentication server which is adapted to: (a) establish a two-way, trusted communication link for access by an authenticated user; (b) where the establishment of the link allows the authenticated user to access a list of application servers; and where (c) the servers are associated with a single client identifier, as in the claims of the present invention.

For at least the above reasons, Appellants assert that claim 1 is not obvious based on the combination of Reed and Palm.

With regard to the remaining Group I claims, dependent claims 2-8, Appellants assert these claims are allowable for the same reason claim 1 is allowable at least because they depend from allowable independent claim 1.

c) Reasons Supporting the Allowability of Group II Claims

(Claims 9-14)

With regard to independent claim 9 from which the remainder of the claims depend, Appellants assert that claim 9 is not obvious in view of the combination of Reed and Palm. Claim 9 reads as follows:

> 9. A method for automatically authenticating a client for a plurality of application servers comprising the steps of:
>
> providing an authentication server;
>
> identifying clients for access to said application servers by said authentication server; and
>
> establishing a two-way trusted communication link between a client and an application server selected from a list of application servers associated with a client identifier.

For purposes of the present Appeal, claim 9 can be viewed as comprising the same elements as claim 1. Therefore, for the reasons set forth above with respect to claim 1, Appellants respectfully submit that claim 9 of the present invention would not have been obvious to one of ordinary skill in the art at the time the invention was filed upon reading the disclosure of Reed or Palm, taken separately or in combination.

With regard to the remaining Group II claims, dependent claims 10-14, Appellants assert that these claims are allowable at least because they depend from allowable independent claim 9.

IX. CONCLUSION

Accordingly, for at least the aforementioned reasons, Appellants respectfully request the Honorable Members of the Board of Patent Appeals and Interferences to reverse each of the

outstanding rejections in connection with the present application and allow each of claims 1-14 to be allowed in connection with the present application.

This Appeal Brief is being presented in triplicate.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No.08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By: _____

John E. Curtin, Reg. No. 37,602
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JEC:psy

Enclosures: Three (3) copies of Appellant's Brief
Appendix -- Clean version of pending claims

APPENDIX A

1. (Previously Presented) An automated authentication handling system for use by clients on a network comprising:

an authentication server adapted to establish a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier.

2. (Previously Presented) The automated authentication handling system of claim 1 wherein said authentication server includes:

an identification engine configured to maintain collections of session assignments for accessing said application servers, each of said session assignment collections being associated with the client identifier.

3. (Original) The automated authentication handling system of claim 2 wherein said identification engine is adapted to receive client identifiers from said clients to establish authenticated users and responsive thereto to provide a user interface to access said application servers according to said associated session assignments.

4. (Previously Presented) The automated authentication handling system of claim 1 wherein said authentication server includes:

a communication initiator engine configured to establish the trusted communication link between said authenticated users and an application server on said list.

5. (Previously Presented) The automated authentication handling system of claim 3 wherein said authentication server includes:

a communication initiator engine configured to establish the trusted communication link defined to one of said session assignments between said authenticated users and said application server.

6. (Original) The automated authentication handling system of claim 1 wherein said session assignments include data fields selected from the group consisting of session timeout and application access level.

7. (Previously Presented) The automated authentication handling system of claim 1 wherein said client identifier includes a user id and password.

8. (Previously Presented) The automated authentication handling system of claim 1 wherein said authentication server includes a processor under the control of software to:

receive an authentication signal from said client;

provide an application access interface to said client in response to said authentication signal; and

establish the trusted communication link between said client and an application server selected from said application access interface.

9. (Previously Presented) A method for automatically authenticating a client for a plurality of application servers comprising the steps of:

providing an authentication server;

identifying clients for access to said application servers by said authentication server; and

establishing a two-way trusted communication link between a client and an application server selected from a list of application servers associated with a client identifier.

10. (Previously Presented) The method of claim 9 wherein said identifying step includes:

providing session parameters for each of said identified clients for at least one of said application servers.

11. (Original) The method of claim 9 wherein said identifying step includes:

providing a user interface to said identified clients for accessing said application servers.

12. (Original) The method of claim 10 wherein said establishing step includes:

using said session parameters to establish said trusted communication link.

13. (Original) The method of claim 11 wherein said user interface includes a listing of application servers and said establishing step is initiated following a selection of an application server by a user from said user interface.

14. (Previously Presented) The method as in claim 1 further comprising a plurality of application servers connected to said network, each requiring authentication for access.

ATTACHMENT A

DRAWINGS

FIG. 1

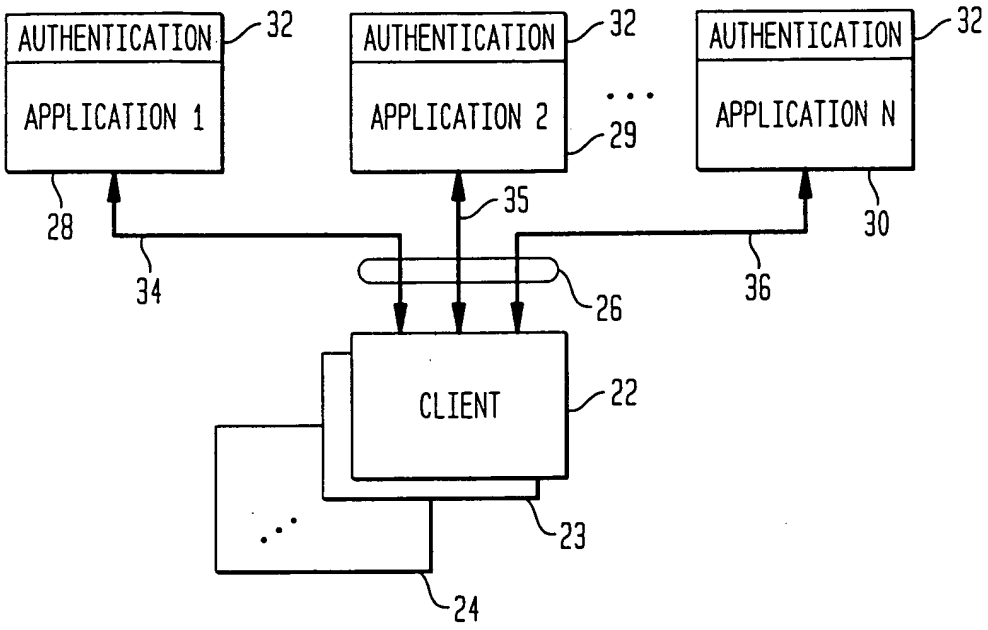

FIG. 2

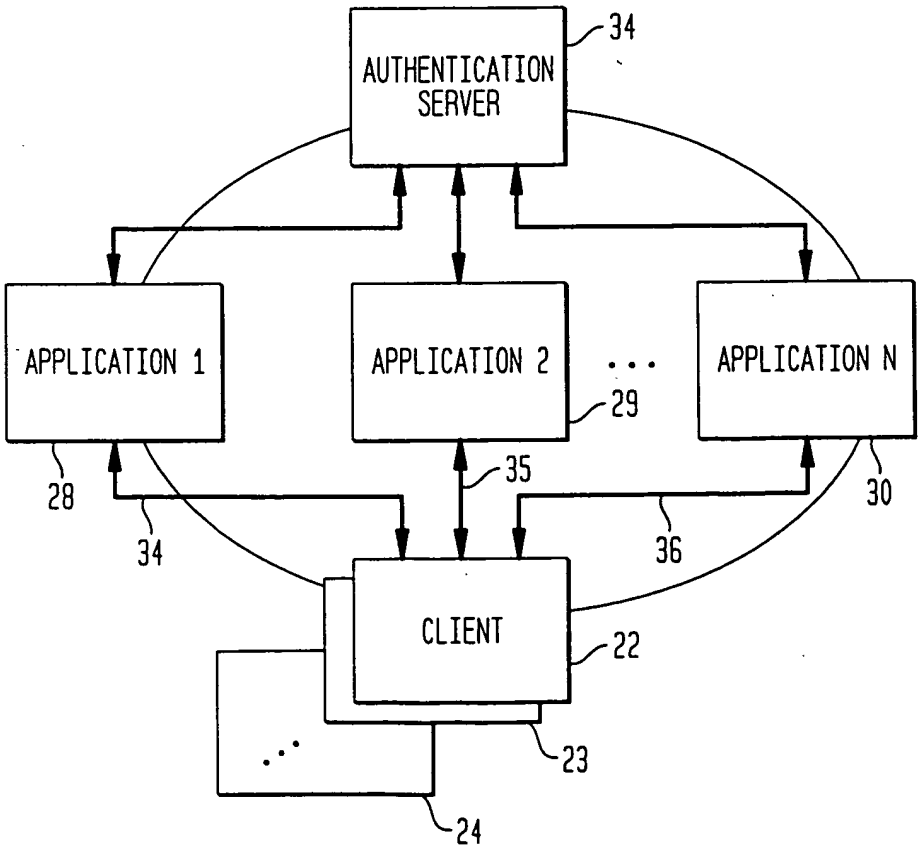

FIG. 3

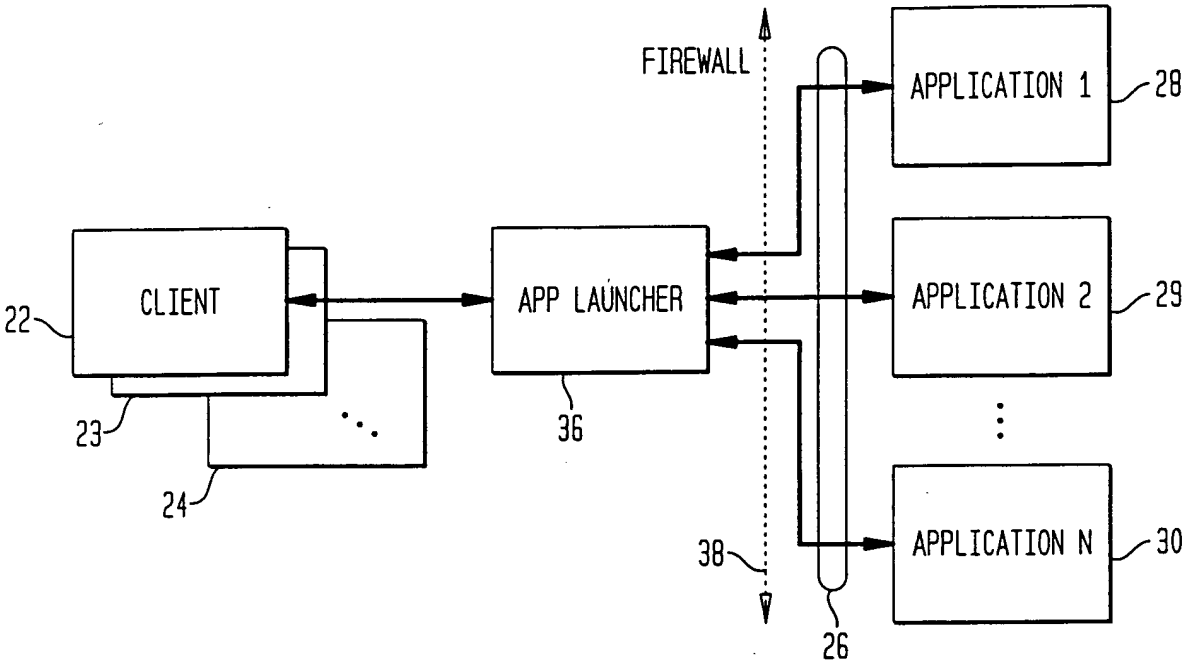

FIG. 4

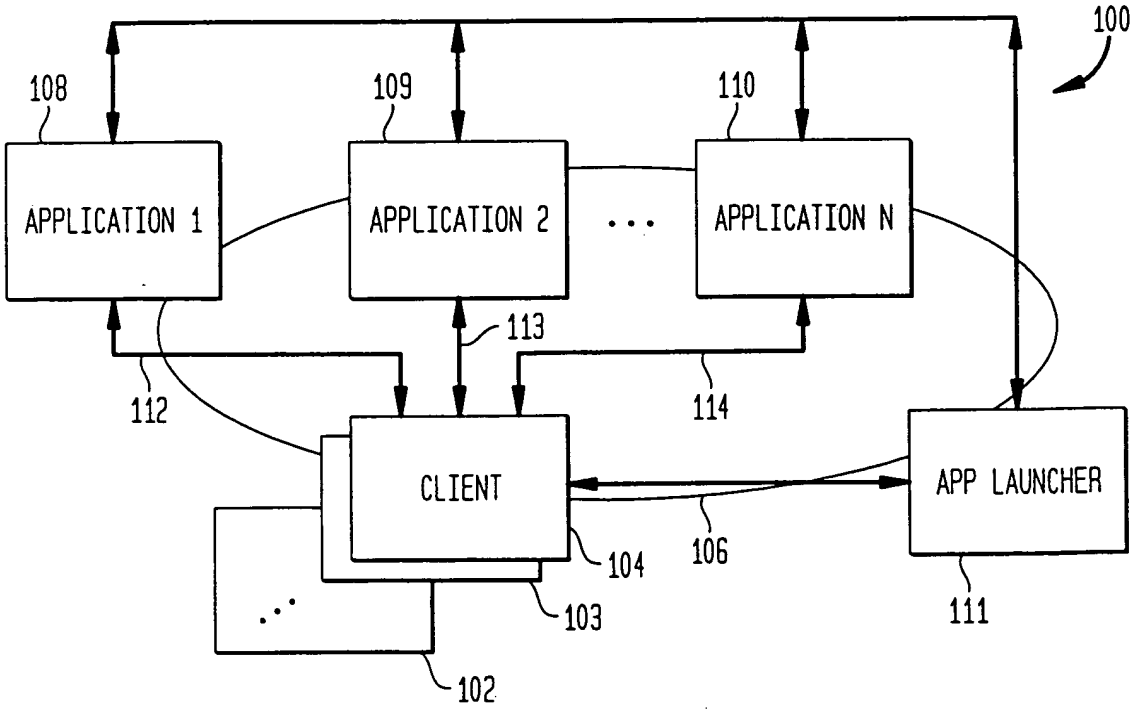

FIG. 5

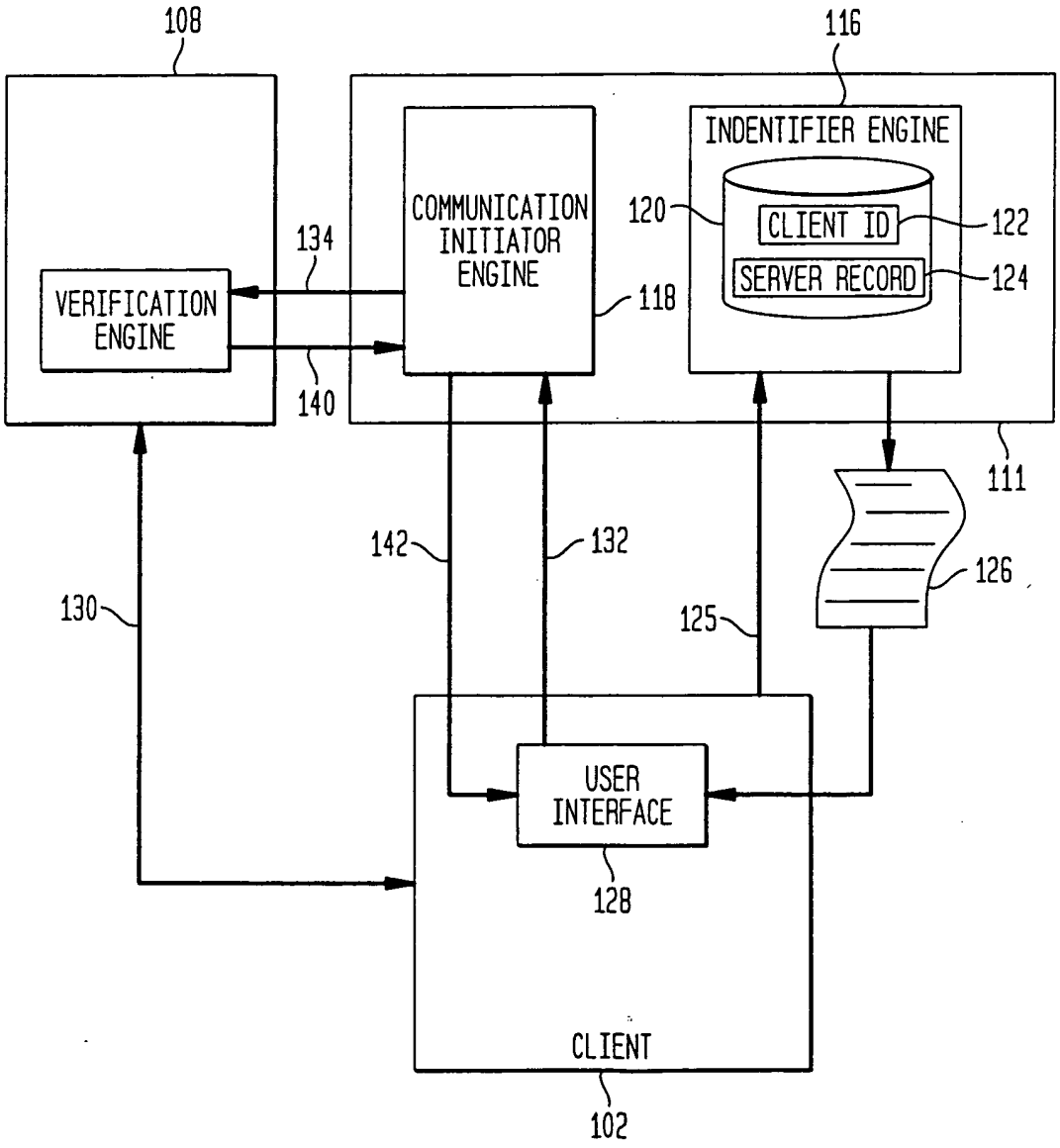

FIG. 6